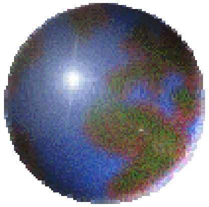
2005 FAA National Software Conference

July 26-28 – Norfolk, Virginia

Component Integration
On Going Research



DTFA03-03-P-10486

Jim Krodel, Pratt Whitney
East Hartford, CT, USA

Sponsoring Org: FAA AIR120/Technical Standards Branch

Outline

- Background of This Research
- Study Considerations
- System Safety Considerations
- Relationship to SC200
- Research Paper Review
- Handbook Review
- Next Phase of Research
- Discussion

Background

- Multi-phased COTS Study Program
  - Phase 1 & 2
    - COTS HW Report (**DOT/FAA/AR-01/41**)
    - COTS SW Report (**DOT/FAA/AR-01/26**)
      - COTS snapshot (nuclear, medical, elev.), Alt methods
      - Emerging COTS – **RTOSs** & Communications
  - Phase 3
    - COTS RTOSs (**DOT/FAA/AR-02/118**)
  - Phase 4
    - COTS RTOSs and architectural considerations
      - (**DOT/FAA/AR-03/77**)

http://www.faa.gov/certification/aircraft/av-info/software/Software%20Research.htm

Background (Cont.)

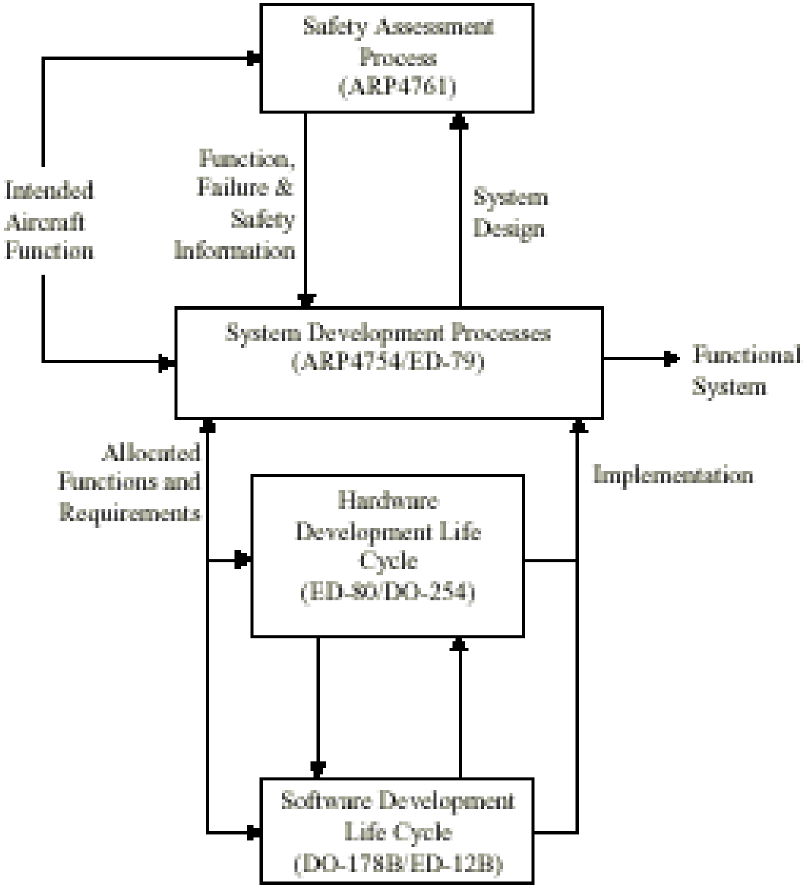
- **Component Integration Study Phases**
  - **Year 1**
    - **Report: "Real Time Operating Systems and Component Integration Considerations for Integration Modular Avionics" – 7/26/04**
  - **Year 2**
    - **Handbook: Integration Considerations in IMA systems – Draft 9/26/05**
  - **Year 3**
    - **Report: Verification Considerations in IMA systems – Draft 7/26/06**

Study contributions by George Romanski of Verocel, Inc.

Component Integration Study

- Attributes
  - Relate to DO-178 and/or DO-278
  - Relate to On-going SC200 Drafts
  - Relate to Current System Safety Disciplines
  - Surveys
    - Literature, Vendors, Applications, Tools, Methods

System Safety Considerations for IMA Systems



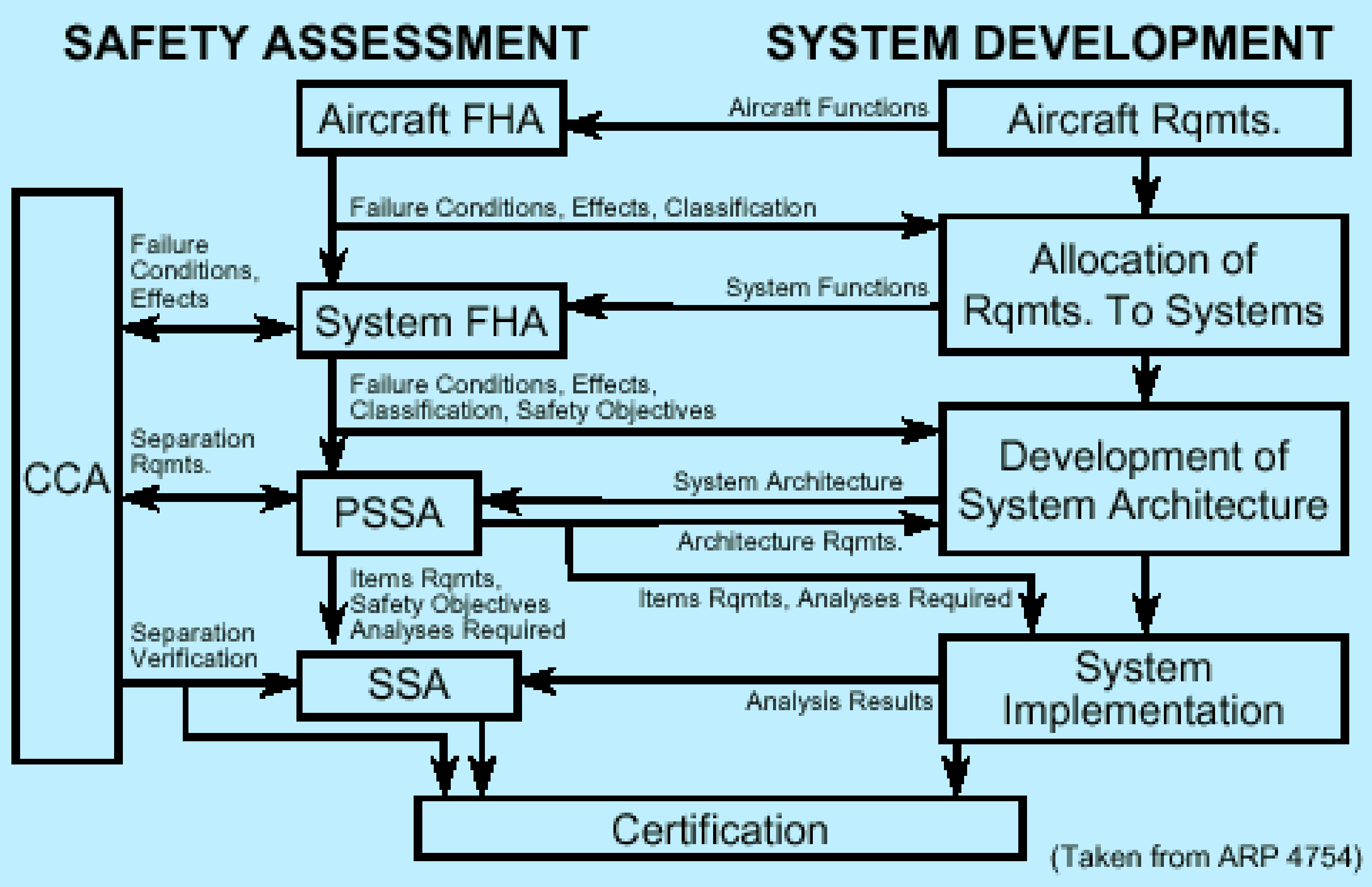
Safety Assessment Process (ARP4761)
Intended Aircraft Function
Function, Failure & Safety Information
System Design
System Development Processes (ARP4754/ED-79)
Functional System
Allocated Functions and Requirements
Implementation
Hardware Development Life Cycle (ED-80/DO-254)
Software Development Life Cycle (DO-178B/ED-12B)

ARP 4754

Federated Look

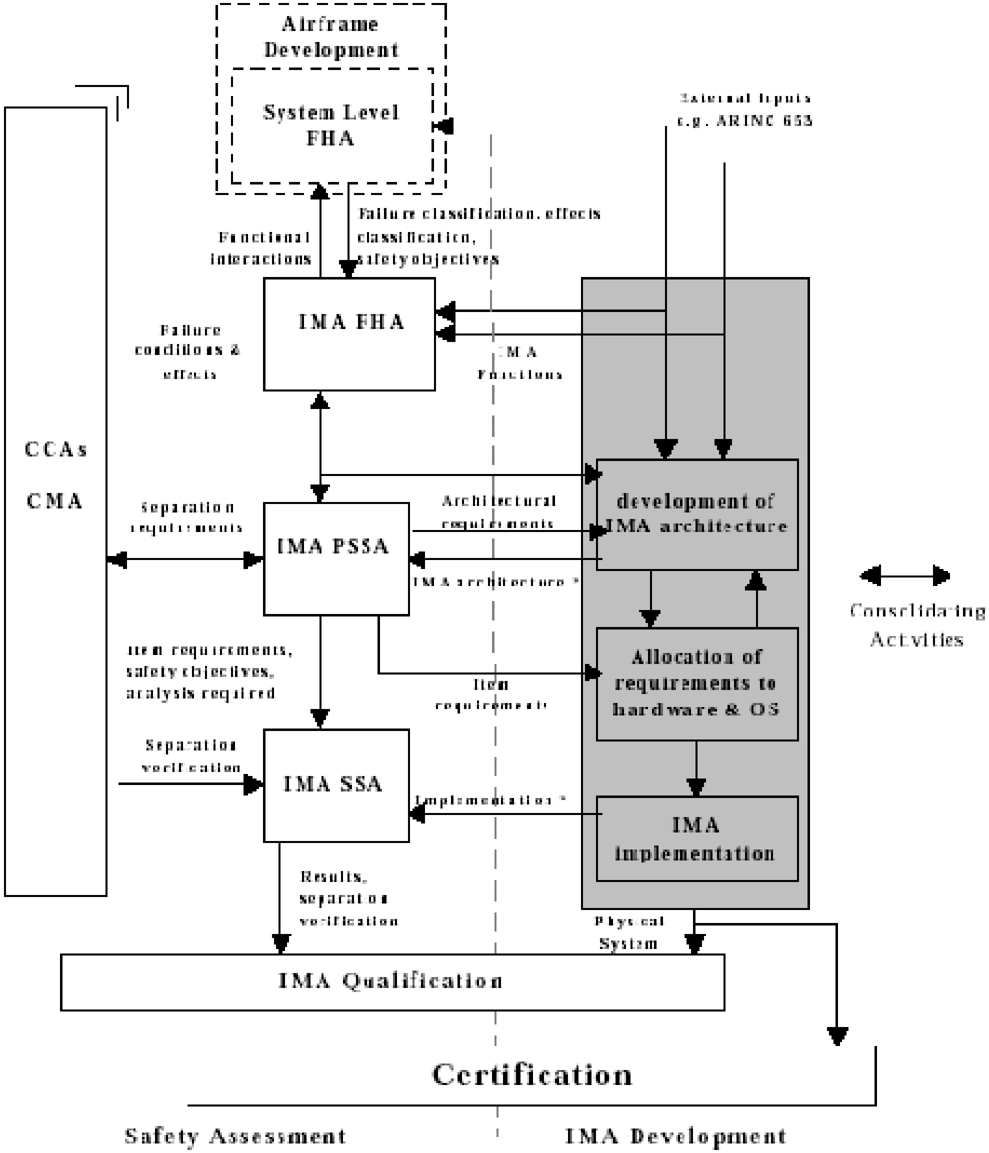
ARP 4754 discusses the steps to develop a system with a proper system safety basis. This document was developed from a federated system mind-set.

IMA Safety Considerations

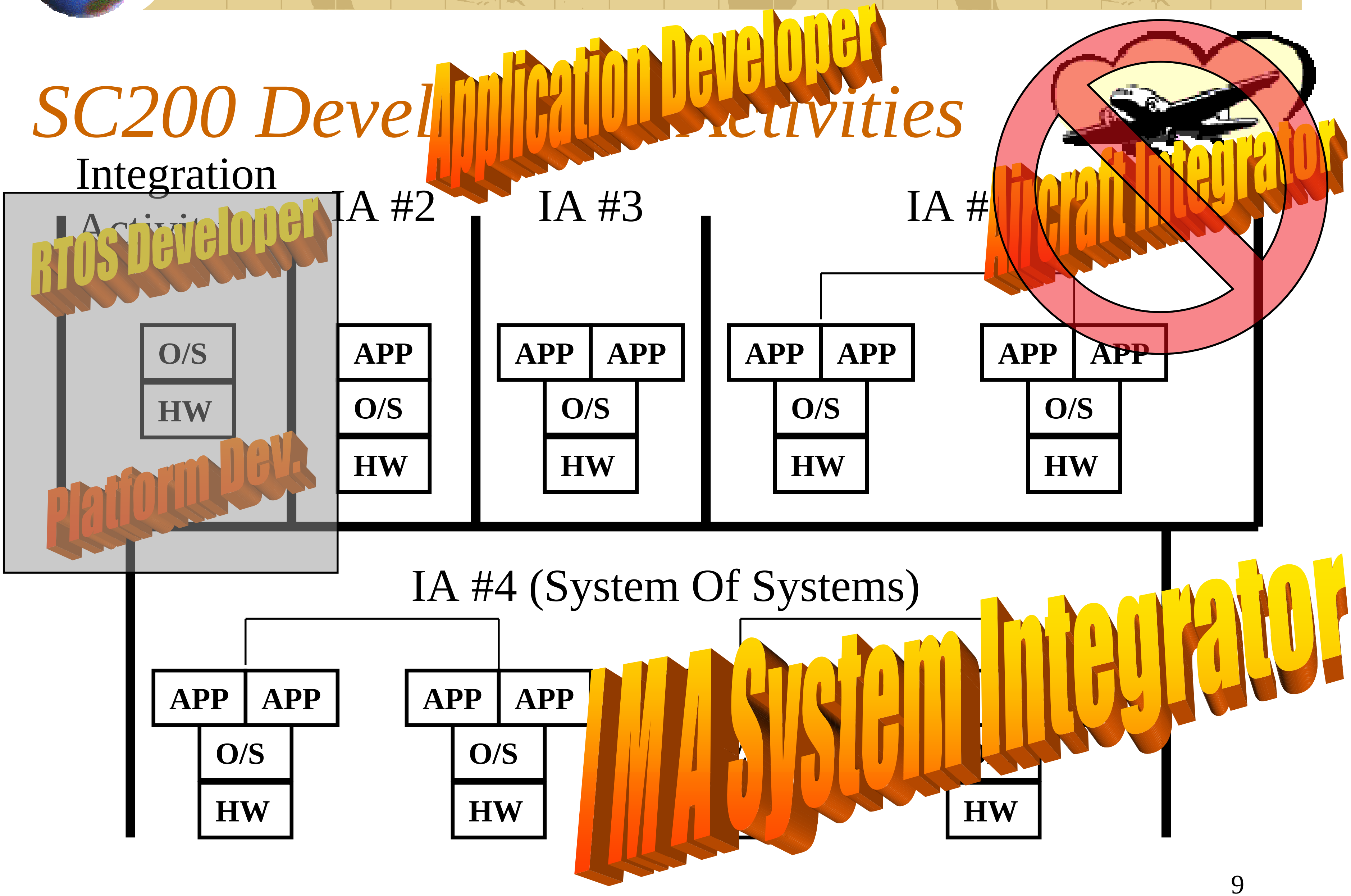

SAFETY ASSESSMENT
SYSTEM DEVELOPMENT
Aircraft FHA
Aircraft Functions
Aircraft Rqmts.
Failure Conditions, Effects, Classification
Allocation of Rqmts. To Systems
Failure Conditions, Effects
System FHA
System Functions
CCA
Failure Conditions, Effects, Classification, Safety Objectives
Separation Rqmts.
Development of System Architecture
PSSA
System Architecture
Architecture Rqmts.
Items Rqmts, Safety Objectives Analyses Required
Items Rqmts, Analyses Required
Separation Verification
SSA
Analysis Results
System Implementation
Certification

(Taken from ARP 4754)

ARP4754 – IMA Mapping



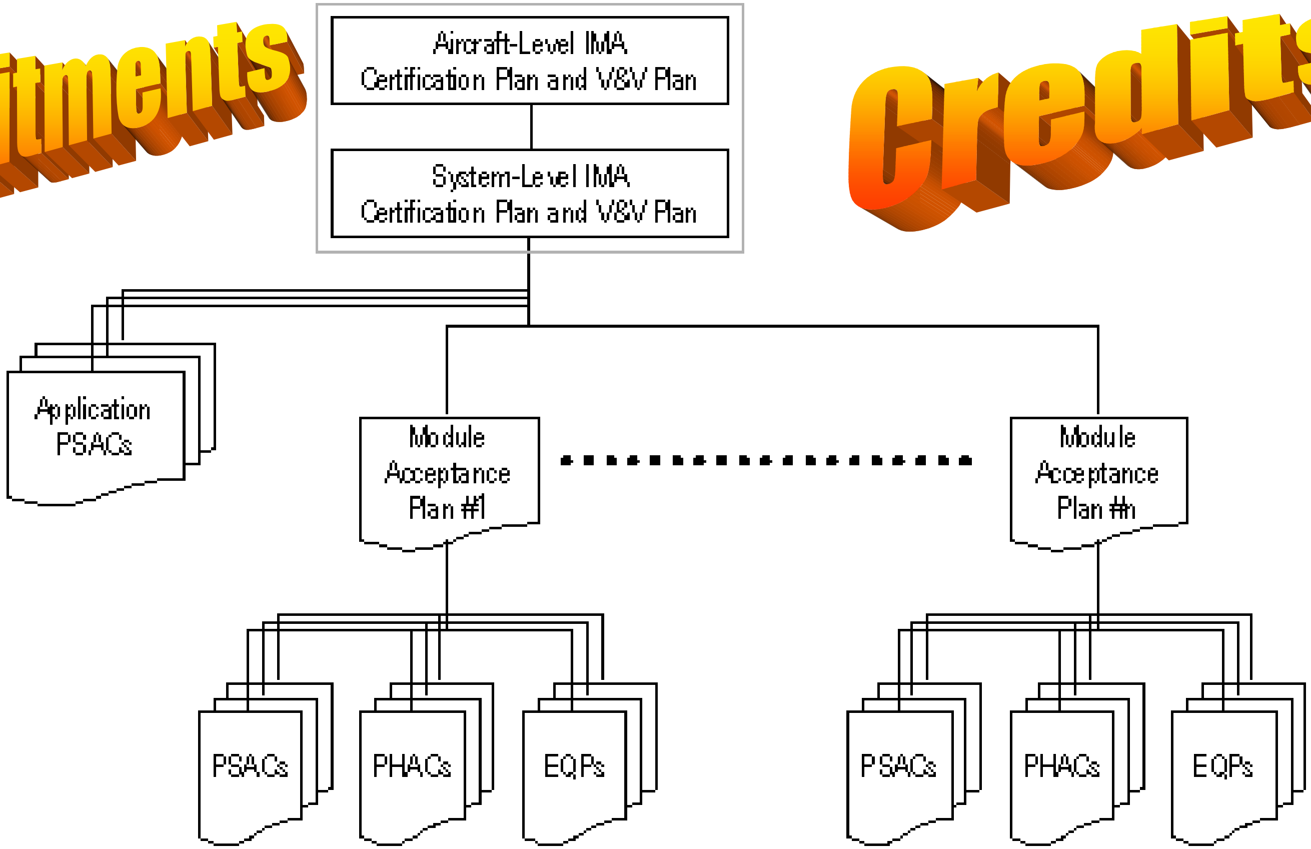
SC200 Development Activities



SC200 Planning Data Schema

Commitments

Credits

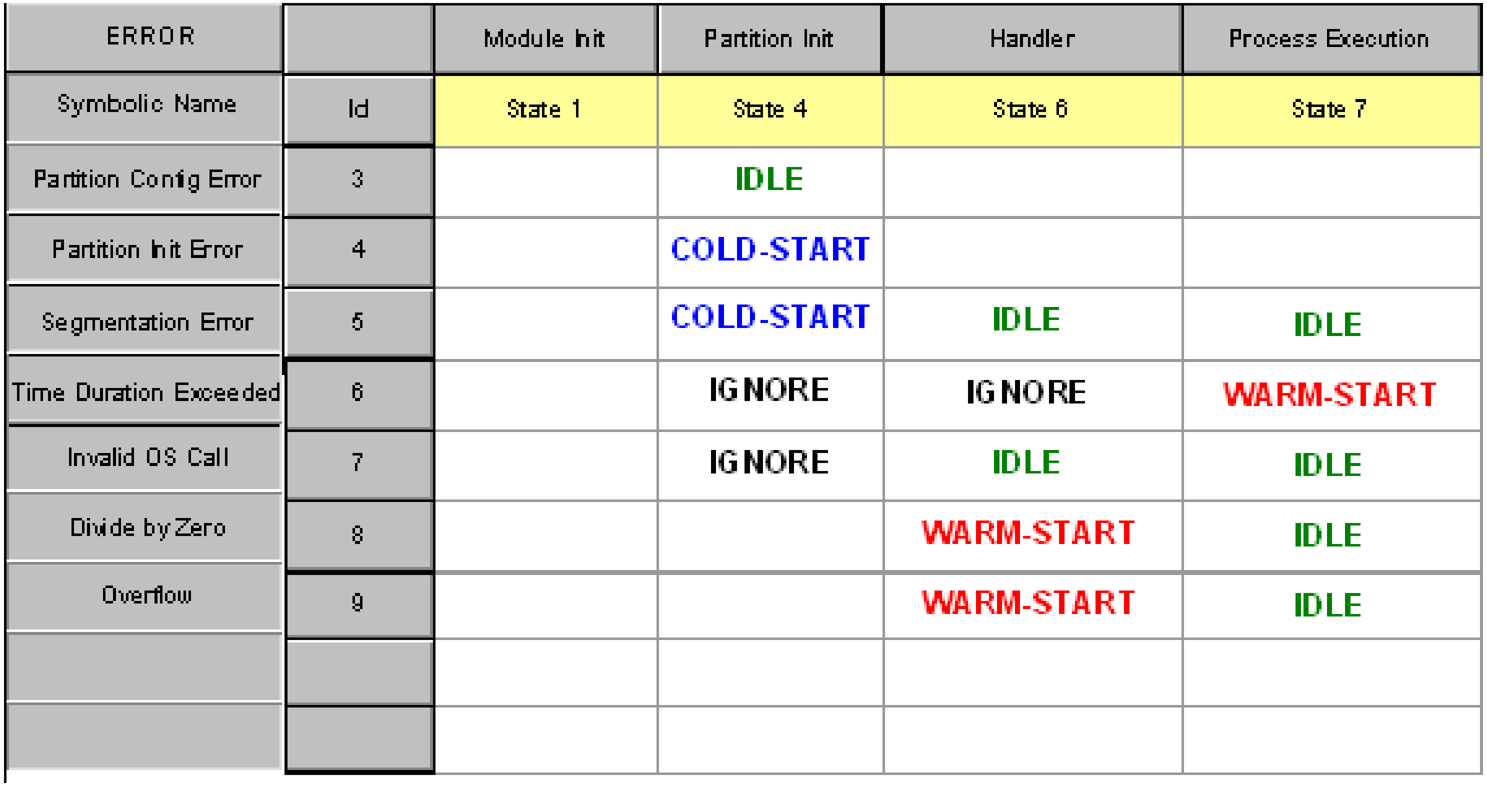


EQP – Environment Qual Plan

Forms of Commitments

Partition Health Management

Health Monitoring Responses to Errors at the Partition Level



ERROR		Module Init	Partition Init	Handler	Process Execution
Symbolic Name	Id	State 1	State 4	State 6	State 7
Partition Config Error	3		IDLE		
Partition Init Error	4		COLD-START		
Segmentation Error	5		COLD-START	IDLE	IDLE
Time Duration Exceeded	6		IGNORE	IGNORE	WARM-START
Invalid OS Call	7		IGNORE	IDLE	IDLE
Divide by Zero	8			WARM-START	IDLE
Overflow	9			WARM-START	IDLE

Research Paper – Review Phase I

- RTOS CONSIDERATIONS IN IMA SYSTEMS
  - Shared Resources and Resource Management
  - IMA Schedulers
  - Run Time Kernels
  - Non-partitioning Run time Operating Systems
  - RTOS within a partition of an IMA system
  - RTOS Exception Handling

Research Paper – Review Phase I

- Integration
- Installation
- Configuration
- Initialization
- System Health Monitoring & Recovery

Handbook Review of Phase II

- Handbook Considerations
  - AC 20-145: Guidance for Integrated Modular Avionics (IMA) that Implement TSO-C153 Authorized Hardware Elements
    - Roles in AC 20-145 are the primarily applicant and FAA.
  - AC 20-148: Guidance for Reusable Component Developers
  - SC-200 - Draft Consensus
  - IMA Experience – Vendor Interviews
  - Published Works

Handbook Review of Phase II

- Handbook
  - Handbook “checklists” or “worksheets” requested
    - Ensure Completeness
  - Not advocates of checklists or worksheets.
    - Handbook as a resource
    - Various Roles - develop own approaches
  - SC-200 requests an IMA certification plan.
    - IMASCP
      - roles defined

Handbook – Review Phase II

- "HANDBOOK FOR COMPONENT INTEGRATION IN IMA SYSTEMS"
  - The Integration Process
    - Roles & Responsibilities
  - Integration Models
    - Set/Use, Communications, etc.
  - Topics of IMA RTOSs & Components

Handbook – Review Phase II

- Topics of IMA RTOSs & Components

Environmental

Hardware

Memory Partitions

Input/Output

Interrupts

Shared Resources

Data

Communications

Process

Time

Identification and Control

Initialization

Installation

Error Handling

Review of Phase II

- Handbook
  - Integration Changes
  - SC200 Roles
    - Certification Authority
    - Certification Applicant
    - IMA System Integrator
    - Platform and Module Suppliers
    - Application Supplier
    - Maintenance Organization
  - Handbook Roles
    - RTOS Developer added

A Peek At the Handbook

- INTEGRATION PLANS
  - FOR COMPONENTS
  - FOR MODULES
  - FOR OVERALL SYSTEM
- INTEGRATION REQUIREMENTS
- INTEGRATION DESIGN
- INTEGRATION VERIFICATION
  - Phase III

A Peek At the Handbook

- PRODUCT CHANGE ACTIVITIES
- IMA INTEGRATION PRACTICES.
    - Set/Use. (Traceability)
    - Worst Case Execution Time.
    - Communications.
    - Integration Models.
- CM FOR THE INTEGRATOR
    - All CM Components [platform, application, rtos, etc]
    - CM in phases
        - Initial, Dev, Verification, Delivery

A Peek At the Handbook

- Data Loader
  - Entire IMA, Single Partition, Single App, IMA, Electronic labeling
- Health Management Systems
  - Monitoring
  - Detection
  - Accommodation functions
- Trial integration

A Peek At the Handbook

- IMA INTEGRATION TOOLS
  - Tool Classes
  - Traceability Tools
  - Modeling Tools Frameworks
  - Configuration Control
  - Data Coupling, Control Coupling

A Peek At the Handbook

- IMA INTEGRATION TOOLS (cont.)
  - Design Integration Environment Tools
  - Modeling Tools
    - Temporal
    - Communication
    - Distributed Target

A Peek At the Handbook

- DOWNSIDES TO CONDSIDER
  - SSA OF FEDERATED VS. IMA
    - FINGER POINTING
  - WCET
  - VERIFICATION PITFALLS
  - REUSE PITFALLS
  - SECURITY

Next Phase of Research

- Year 2
  - Handbook: Integration Considerations in IMA systems – Draft 9/26/05
- Year 3
  - Report: Verification Considerations in IMA systems – Draft 7/26/06
- Contributions From Attendees Welcome
  - james.krodel@pw.utc.com

- **james.krodel@pw.utc.com**